UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/864,136	05/24/2001	Ajit Clarence D'Sa	AUS9-2000-0936-US1	1089

7590 08/16/2004

Joseph T. Van Leeuwen
P.O. Box 81641
Austin, TX 78708-1641

EXAMINER	
BAUM, RONALD	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 08/16/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/864,136	D'SA ET AL.	
	Examiner	Art Unit	
	Ronald Baum	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-20 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-20 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-20 are pending for examination.

2. Claims 1-20 are rejected.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 19 recites the limitation " A computer program product ... claim 5". There is insufficient antecedent basis for this limitation in the claim. The examiner assumes for the sake of applying art that the "claim 5" phrase should be "claim 18".

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1-20 are rejected under 35 U.S.C. 102(b) as being anticipated by Minear et al, U.S. Patent 5,983,350.

4. As per claim 1; "A method of establishing a secure communication path between a computer system and a remote computer system comprising: exchanging identification data with the remote computer system using a communication path [col. 3,lines 35-col. 18,line 48]; determining, based on the identification data, whether a predefined security policy exists

corresponding to the remote computer system [col. 3,lines 35-col. 18,line 48, whereas the SA aspects of IPSEC parameters clearly associate remote host identification data to communications security policy.]; and establishing a secure communication path using a default security policy in response to determining that the predefined security policy does not exist [col. 3,lines 35-col. 18,line 48, whereas the different levels of security, insofar as the setup of boot default values, constitutes a default protection level for establishing secure communication.].";

Further, as per claim 8; "An information handling system [This claim is the apparatus claim for the method claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection] comprising: one or more processors; a memory accessible by the processors; a nonvolatile storage accessible by the processors; a network interface connecting the information handling system to a computer network; and a network tool for creating a secure communication path to a remote computer system, the network tool including: means for exchanging identification data with the remote computer system using a communication path; means for determining, based on the identification data, whether a predefined security policy exists corresponding to the remote computer system; and means for establishing a secure communication path using a default security policy in response to determining that the predefined security policy does not exist.";

Further, as per claim 14; "A computer program product stored on a computer operable medium [This claim is the software computer-readable medium claim for the method claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection] for establishing a secure communication path between a computer system and a remote computer system comprising: means for exchanging identification data with the remote computer system using a

communication path; means for determining, based on the identification data, whether a predefined security policy exists corresponding to the remote computer system; and means for establishing a secure communication path using a default security policy in response to determining that the predefined security policy does not exist.".

5. Claim 2 ***additionally recites*** the limitation that; "The method as described in claim 1 wherein the identification data is selected from the group consisting of a gateway address, a host name, a user identifier, an IP address, and a distinguished name.". The teachings of Minear et al suggest such limitations (col. 3,lines 35-col. 18,line 48, whereas the SA aspects of IPSEC parameters clearly associate remote host identification data to a gateway (i.e., firewall) address, a host name, a user identifier, or an IP address.);

Further, as per claim 9 ***additionally reciting*** the limitation that; "The information handling system [This claim is the apparatus claim for the method claim 2 above, and is rejected for the same reasons provided for the claim 2 rejection] as described in claim 8 wherein the identification data is selected from the group consisting of a gateway address, a host name, a user identifier, an IP address, and a distinguished name.";

Further, as per claim 15 ***additionally reciting*** the limitation that; "The computer program product [This claim is the software computer-readable medium claim for the method claim 2 above, and is rejected for the same reasons provided for the claim 2 rejection] as described in claim 14 wherein the identification data is selected from the group consisting of a gateway address, a host name, a user identifier, an IP address, and a distinguished name.".

6. Claim 3 ***additionally recites*** the limitation that; "The method as described in claim 1 wherein establishing the secure communication path further includes: determining whether a digital certificate or a pre-shared key is used for encrypting data.". The teachings of Minear et al suggest such limitations (col. 3,lines 35-col. 18,line 48, whereas the SA aspects of IPSEC parameters clearly associate remote host secure communications to pre-shared key data (i.e., DES, MD5 transform functions/protocols) used for encrypting/decrypting data.);

Further, as per claim 10 ***additionally reciting*** the limitation that; "The information handling system [This claim is the apparatus claim for the method claim 3 above, and is rejected for the same reasons provided for the claim 3 rejection] as described in claim 8 wherein the means for establishing the secure communication path further] includes: means for determining whether a digital certificate or a pre-shared key is used for encrypting data.";

Further, as per claim 16 ***additionally reciting*** the limitation that; "The computer program product [This claim is the software computer-readable medium claim for the method claim 3 above, and is rejected for the same reasons provided for the claim 3 rejection] as described in claim 14 wherein the means for establishing the secure communication path further includes: means for determining whether a digital certificate or a pre-shared key is used for encrypting data.".

7. Claim 4 ***additionally recites*** the limitation that; "The method as described in claim 1 further comprising: searching a group table for a group identifier corresponding to the remote computer system; wherein the predefined security policy corresponds to the group identifier in response to a successful group identifier search.". The teachings of Minear et al suggest such

limitations (col. 3,lines 35-col. 18,line 48, whereas the SA database and searches of such for identification to database entry matches clearly associate remote host identifier (corresponding to the remote computer system) to assigned SA/security policy for the secure communication path.);

Further, as per claim 11 ***additionally reciting*** the limitation that; "The information handling system [This claim is the apparatus claim for the method claim 4 above, and is rejected for the same reasons provided for the claim 4 rejection] as described in claim 8 further comprising: means for searching a group table for a group identifier corresponding to the remote computer system; wherein the predefined security policy corresponds to the group identifier in response to a successful group identifier search.";

Further, as per claim 17 ***additionally reciting*** the limitation that; "The computer program product [This claim is the software computer-readable medium claim for the method claim 4 above, and is rejected for the same reasons provided for the claim 4 rejection] as described in claim 14 further comprising: means for searching a group table for a group identifier corresponding to the remote computer system; wherein the predefined security policy corresponds to the group identifier in response to a successful group identifier search.".

8. Claim 5 ***additionally recites*** the limitation that; "The method as described in claim 1 further comprising: selecting a proposal and transforms corresponding to the default security policy; creating a security association payload using the selected proposal and transforms; and sending the security association from one computer system to the remote computer system.". The teachings of Minear et al suggest such limitations (col. 3,lines 35-col. 18,line 48, whereas the SA

aspects of IPSEC parameters clearly associate remote host secure communications establishment via the security protocol handshaking (i.e., cross transfer of transform types, identification, etc., as part of the payload transferred between the hosts), and whereas the different levels of security, insofar as the setup of boot default values, constitutes a default protection level for establishing said secure communication.);

Further, as per claim 12 ***additionally reciting*** the limitation that; "The information handling system [This claim is the apparatus claim for the method claim 5 above, and is rejected for the same reasons provided for the claim 5 rejection] as described in claim 8 further comprising: means for selecting a proposal and transforms corresponding to the default security policy; means for creating a security association payload using the selected proposal and transforms; and means for sending the security association from one computer system to the remote computer system.";

Further, as per claim 18 ***additionally reciting*** the limitation that; "The computer program product [This claim is the software computer-readable medium claim for the method claim 5 above, and is rejected for the same reasons provided for the claim 5 rejection] as described in claim 14 further comprising: means for selecting a proposal and transforms corresponding to the default security policy; means for creating a security association payload using the selected proposal and transforms; and means for sending the security association from one computer system to the remote computer system.".

9. Claim 6 ***additionally recites*** the limitation that; "The method as described in claim 5 further comprising: receiving a response from the remote computer system; determining whether

the proposal was accepted by the other computer system; and verifying identification information in response to the proposal being accepted.". The teachings of Minear et al suggest such limitations (col. 3,lines 35-col. 18,line 48, whereas the SA aspects of IPSEC parameters clearly associate remote host secure communications establishment via the security protocol handshaking clearly encompasses an acknowledgement feedback message which constitutes verification of proposal acceptance.);

Further, as per claim 13 ***additionally reciting*** the limitation that; "The information handling system [This claim is the apparatus claim for the method claim 6 above, and is rejected for the same reasons provided for the claim 6 rejection] as described in claim 12 further comprising: means for receiving a response from the remote computer system; means for determining whether the proposal was accepted by the other computer system; and means for verifying identification information in response to the proposal being accepted.";

Further, as per claim 19 ***additionally reciting*** the limitation that; "The computer program product [This claim is the software computer-readable medium claim for the method claim 6 above, and is rejected for the same reasons provided for the claim 6 rejection] as described in claim ***18*** further comprising: means for receiving a response from the remote computer system; means for determining whether the proposal was accepted by the other computer system; and means for verifying identification information in response to the proposal being accepted.".

10. Claim 7 ***additionally recites*** the limitation that; "The method as described in claim 1 further comprising: verifying a remote identifier and a digital signature corresponding to the remote computer system; and creating the secure communication path to the remote computer

system in response to the verification.". The teachings of Minear et al suggest such limitations (col. 3,lines 35-col. 18,line 48, whereas the SA aspects of IPSEC parameters clearly associate remote host secure communications establishment via the security protocol handshaking clearly encompasses an acknowledgement verifying a remote identifier and a digital signature via the MD5 authentication protocol aspect of the IPSEC.);

Further, as per claim 20 ***additionally reciting*** the limitation that; "The computer program product [This claim is the software computer-readable medium claim for the method claim 7 above, and is rejected for the same reasons provided for the claim 7 rejection] as described in claim 14 further comprising: means for verifying a remote identifier and a digital signature corresponding to the remote computer system; and means for creating the secure communication path to the remote computer system in response to the verification".

Conclusion

11. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (703) 305-4276. The examiner can normally be reached Monday through Friday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (703) 305-9648. The Fax numbers for the organization where this application is assigned are:

After-final	(703) 746-7238
Official	(703) 746-7239
Non-Official/Draft	(703) 746-7246

Ronald Baum

Patent Examiner

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100